Unified Wireless Network ローカル EAP サーバ の設定例

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 Cisco Wireless LAN Controller でのローカル EAP の設定 ローカル EAP の設定 **Microsoft Certification Authority** 設置 Cisco Wireless LAN Controller での証明書のインストール Wireless LAN Controller でのデバイス証明書のインストール Wireless LAN Controller へのベンダー CA 証明書のダウンロード EAP-TLS を使用するための Wireless LAN Controller の設定 クライアント デバイスへの認証局証明書のインストール クライアント用ルート CA 証明書のダウンロードとインストール クライアント デバイス用のクライアント証明書の生成 クライアント デバイス上での Cisco Secure Services Client による EAP-TLS の指定 デバッグ コマンド 関連情報

<u>概要</u>

このドキュメントでは、ワイヤレス ユーザの認証のために Cisco Wireless LAN Controller(WLC)でローカル拡張認証プロトコル(EAP)サーバを設定する方法について説明し ます。

ローカル EAP は認証方法であり、これを使用して、ユーザとワイヤレス クライアントをローカ ルに認証できます。この機能は、バックエンド システムが中断したり外部認証サーバが停止した りした場合でもワイヤレス クライアントとの接続を維持する必要があるリモート オフィスでの使 用を想定して作られています。ローカル EAP を有効にすると、コントローラは認証サーバおよび ローカル ユーザ データベースとして機能するため、外部認証サーバへの依存が排除されます。ロ ーカル EAP は、ローカル ユーザ データベースまたは Lightweight Directory Access Protocol (LDAP) バックエンド データベースからユーザ クレデンシャルを受け取り、ユーザを 認証します。ローカル EAP は、コントローラとワイヤレス クライアント間で Lightweight EAP (LEAP)、EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) および EAP-Transport Layer Security (EAP-TLS) 認証をサポートします。

ローカル EAP サーバは、WLC にグローバル外部 RADIUS サーバ設定がある場合だけ使用できま

せん。すべての認証要求は、ローカル EAP サーバが使用可能になるまで、グローバル外部 RADIUS サーバに転送されます。WLC が外部 RADIUS サーバとの接続を失うと、ローカル EAP サーバがアクティブになります。グローバル RADIUS サーバ設定がない場合、ローカル EAP サ ーバはすぐにアクティブになります。ローカル EAP サーバは、他の WLC に接続されている、ク ライアントの認証に使用できません。つまり、WLC は、認証のために別の WLC に EAP 要求を 転送できません。すべての WLC には、その独自のローカル EAP サーバと個別データベースが必 要です。

注:WLCが外部RADIUSサーバ(ACS)に要求を送信するのを停止するには、次のコマンドを使用 します。

```
config wlan disable
config wlan radius_server auth disable
config wlan enable
```

ローカル EAP サーバは、次のプロトコルを 4.1.171.0 ソフトウェア リリース以降で使用します。

- LEAP
- EAP-FAST(ユーザ名とパスワードの両方および証明書)
- EAP-TLS

<u>前提条件</u>

<u>要件</u>

次の項目に関する知識があることが推奨されます。

- WLC と Lightweight アクセス ポイント(LAP)の基本動作のための設定方法に関する知識
- Lightweight アクセス ポイント プロトコル(LWAPP)とワイヤレスのセキュリティ方式に関する知識
- ローカル EAP 認証に関する基礎知識

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CB21AG アダプタ カードと Cisco Secure Services Client バージョン 4.05 を伴う Windows XP
- Cisco 4400 Wireless LAN Controller 4.1.171.0
- Microsoft Certification Authority (Windows 2000 $\forall -N$)

<u>表記法</u>

ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法』を参照してください。</u>

<u>Cisco Wireless LAN Controller でのローカル EAP の設定</u>

このドキュメントでは、WLC の基本的な設定がすでに完了していることが想定されています。

<u>ローカル EAP の設定</u>

ローカル EAP を設定するには、次の手順を実行します。

1. ローカル ネット ユーザを追加するには、次の手順を実行します。GUIから、[Security] > [Local Net Users] > [New] を選択し、[User Name]、[Password]、[Guest User]、[WLAN ID]、および[Description]を入力して、[Apply]をクリックします。

11 111 11				00 <u>T</u> 0 00	anigereson E	ing codence Wenters
cisco	MONITOR WLANS <u>C</u> (ONTROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	Local Net Users > Ne	9W			< Back	Apply
General	User Name	eapuser2				
Authentication Accounting	Password	*******				
IDAP	Confirm Password	•••••				
Local Net Users MAC Filtering Disabled Clients	Guest User					
User Login Policies AP Policies	WLAN ID	1				
Local EAP General	Description	Employee user local datab	ase			

CLIから、**config netuser add** *<username> <password> <WLAN id> <description>コマンドを* 使用できます。注:このコマンドは、スペースの制約により2行にわたって表記されていま す。

(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database

2. ユーザ クレデンシャルの取得順を指定します。GUI から、[Security] > [Local EAP] > [Authentication Priority] を選択します。次に、[LDAP]を選択し、[<**]ボタンを**クリックして [**Apply**]をクリ**ックします**。これにより、まずユーザ クレデンシャルがローカル データベー スに置かれます。

li.ili. cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HErb
Security	Priority 0	rder > L	ocal-Auth					
General	User Cred	lentials						
Authentication Accounting TACACS+ Authentication Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	LDAP	<	LOCAL U	P WN				-
▼ Local EAP Profiles EAP-FAST Parameters Authentication Priority								

CLIから、

(Cisco Controller) >config local-auth user-credentials local

3. EAP プロファイルを追加します。これを GUI から行うには、[Security] > [Local EAP] > [Profiles] を選択して、[New] をクリックします。新しいウィンドウが表示されたら、[Profile Name] を入力して、[Apply] をクリックします。

-	MONITO	DR	<u>W</u> LANS	CONTROLL	ER WIR	ELESS S	ECURITY	MANA	GEMENT	COMMANDS	HEU	P
	Local	EAP	Profiles									New Apply
	Profile	Nan	ie .		LEAP	EAP-I	AST		EAP-TI	.5		1
												•
rs												
ty												
HOLE	100 W.		004750115	 with cost 			1517 CO		LEID			Sage Configuration Bing Logout Bethe
Tour		413 afiles	- New	v ulkeres	gecowin	- Alento	-04 C <u>V</u>		ney.			
roc3	I EAP PI	onies	> 146M			_						< sack Apply
Profil	e Name					EAP	Hest					

これは、CLI コマンド config local-auth eap-profile add <profile-name> を使用して行うこと もできます。 この例では、プロファイル名は EAP-test です。 (Cisco Controller) >config local-auth eap-profile add EAP-test

4. 方式を EAP プロファイルに追加します。GUI から、[Security] > [Local EAP] > [Profiles] を 選択して、認証方式を追加するプロファイル名をクリックします。この例では、LEAP、 EAP-FAST および EAP-TLS を使用します。[Apply] をクリックして、方式を設定します。

.ili.ili. cisco	MONITOR MLANS CONTROLLER WIRELESS	SECURITY NAVAGEMENT COMMANDS HELP	
Security	Local EAP Profiles		
Ceneral PADOUS	Profile Name LEAP EAR-cest IP	EAP-TAST EAP-TLS	
cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP	
Security	Local EAP Profiles > Edit		
- AAA	Profile Name	EAP-test	
RADIUS Authentication	LEAP		
Accounting • TACACS+ LDAR	EAP-FAST	P	
Local Net Users MAC Filtering	EAP-TLS	P	
Disabled Clients User Login Policies AP Policies	Local Certificate Required	P Enabled	
* Local EAP	Client Certificate Required	P Enabled	
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor V	
Authentication Priority Priority Order	Check against CA certificates	P Enabled	
♦ Access Central Lists	Verify Certificate CN Identity	Enabled	
+ IPSec Certs		E com	
Wireless Protection Delicies	Check Certificate Date Validity	L. Enabled	

CLIコマンドconfig local-auth eap-profile method add *<method-name> <profile-name>を使用 できます*。この設定例では、3 つの方式をプロファイル EAP-test に追加します。追加する 方式は、LEAP、EAP-FAST および EAP-TLS で、名前はそれぞれ *leap、fast* および *tls* です 。次に、CLI コンフィギュレーション コマンドの出力を示します。 (Cisco Controller) >config local-auth eap-profile method add leap EAP-test (Cisco Controller) >config local-auth eap-profile method add fast EAP-test (Cisco Controller) >config local-auth eap-profile method add tis EAP-test 5. EAP 方式のパラメータを設定します。これは、EAP-FAST だけで使用されます。設定する パラメータは次のとおりです。[Server Key (server-key)]: Protected Access Credential (PAC) (16 進数)を暗号化/復号化するサーバ キー。[Time to Live for PAC (pac-ttl)]: PAC の存続可能時間を設定します。[Authority ID (authority-id)]: 任意 ID を設定し ます。[Annonymous Provision (anon-provn)]: 匿名プロビジョニングを許可するかどうかを 設定します。このコマンドはデフォルトで有効になっています。GUI から設定する場合、 [Security] > [Local EAP] > [EAP-FAST Parameters] を選択して、[Server key]、[Time to live for the PAC]、[authority ID (in hex)] および [Authority ID Information] の値を入力します。

Bouriou Woods 74	oreinousen regression	geconant regenoenen	Conversion and	
EAP-FAST Method Pa	arameters			
Server Key (in hex)			****	
Confirm Server Key			****	
Time to live for the PA	iC .		10 days	
Authority ID (in hex)			436973636f	
Authority ID Informati	ion		Cisce A-ID	
Anonymous Provision			F Enabled	

次に、これらの EAP-FAST のパラメータを設定するときに使用する CLI コンフィギュレー ション コマンドを示します。

(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10

6. WLAN でのローカル認証を有効にします。GUI から、トップ メニューの [WLANs] を選択し 、ローカル認証を設定する WLAN を選択します。新しいウィンドウが表示されます。

[Security] > [AAA] タブをクリックします。[Local EAP authentication] チェックボックスをオ ンにして、この例に示すように、プルダウン メニューから正しい EAP プロファイル名を選 択します。

uludu cisco	MONETOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HEL	,
WLANs	WLANs > Edit General Security QoS Advanced	
 WLANS WLANS AP Groups VLAN 	Layer 2 Layer 3 AAA Servers Select AAA servers below to override use of default servers on this WLAN Radius Servers Radius Servers Authentication Servers	LDAP Servers Server 1 None
	Server 1 None Server 2 None Server 3 None Local EAP Authentication Local EAP Authentication EAP Profile Name EAP-test #	Server 3 None 🗷

また、次に示すように、CLI config wlan local-auth enable *<profile-name> <wlan-id>設定コ マンドを発行*することもできます。

(Cisco Controller) >config wlan local-auth enable EAP-test 1

7. [Layer 2 Security] パラメータを設定します。GUI インターフェイスから、[WLAN Edit] ウィ ンドウで、[Security] > [Layer 2] タブに移動して、[Layer 2 Security] プルダウン メニューか ら [WPA+WPA2] を選択します。[WPA+WPA2 Parameters] セクションで、[WPA Encryption] を [TKIP]、[WPA2 Encryption] を [AES] に設定します。次に [Apply] をクリック します。

11 11 11		aale counderation Find codoor Venesu
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY N	MANAGEMENT C <u>O</u> MMANDS HELP
WLANS WLANS WLANS AP Groups VLAN	WLANS > Edit General Security Qo5 Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security COSCREWINGS MAC Filtering WPA+WPA2 Parameters WPA Policy WPA Encryption AES TKIP WPA2 Policy WPA2 Encryption PAES TKIP Auth Key Mgmt 802.1X	< Back Apply
CLI から、次のコ゛	マンドを使用します。	

(Cisco Controller) >config wlan security wpa enable 1 (Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1 (Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1

8. 設定を確認します。

(Cisco Controller) >show local-auth config

User credentials database search order: Primary Local DB Timer: Active timeout Undefined Configured EAP profiles: Name EAP-test Certificate issuer cisco Peer verification options: Check against CA certificates Enabled Verify certificate CN identity Disabled Check certificate date validity Enabled EAP-FAST configuration: Local certificate required No Client certificate required No Enabled methods leap fast tls Configured on WLANs 1 EAP Method configuration: EAP-FAST: --More-- or (q)uit Server key <hidden> TTL for the PAC 10 Anonymous provision allowed Yes Authority Information CiscoA-ID wlan 1の特定のパラメータは、**show wlan** *<wlan id>コマンドで確認でき***ます**。

⁽Cisco Controller) >**show wlan 1**

Profile Name..... austinlab Network Name (SSID)..... austinlab Status..... Disabled MAC Filtering..... Disabled Broadcast SSID..... Enabled AAA Policy Override..... Disabled Number of Active Clients..... 0 Session Timeout..... 1800 seconds Interface..... management WLAN ACL..... unconfigured DHCP Server..... Default DHCP Address Assignment Required..... Disabled Quality of Service...... Silver (best effort) WMM..... Disabled CCX - Aironetle Support..... Enabled CCX - Gratuitous ProbeResponse (GPR) Disabled Dot11-Phone Mode (7920)..... Disabled Wired Protocol..... None --More-- or (q)uit IPv6 Support..... Disabled Radio Policy..... All Local EAP Authentication..... Enabled (Profile 'EAP-test') Security 802.11 Authentication:..... Open System Static WEP Keys..... Disabled 802.1X..... Disabled Wi-Fi Protected Access (WPA/WPA2)..... Enabled WPA (SSN IE)..... Enabled TKIP Cipher..... Enabled AES Cipher..... Disabled WPA2 (RSN IE)..... Enabled TKIP Cipher..... Disabled AES Cipher..... Enabled Auth Key Management 802.1x.... Enabled PSK..... Disabled CCKM..... Disabled CKIP Disabled IP Security..... Disabled IP Security Passthru..... Disabled Web Based Authentication..... Disabled --More-- or (q)uit Web-Passthrough..... Disabled Conditional Web Redirect..... Disabled Auto Anchor..... Disabled Cranite Passthru..... Disabled Fortress Passthru..... Disabled H-REAP Local Switching..... Disabled Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled) Client MFP..... Optional Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List

WLAN ID IP Address Status

アクティブ タイムアウト タイマーなど、その他のローカル認証パラメータを設定できます 。このタイマーは、すべての RADIUS サーバで障害が発生した後でローカル EAP が使用さ れる期間を設定します。GUI から、[Security] > [Local EAP] > [General] を選択して、時間値 を設定します。次に [Apply] をクリックします。

սիսիս						Sa <u>v</u> e C	onfiguration <u>F</u>	ing Logout <u>R</u> efres
cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	General					1		Apply
 AAA General RADIUS Authentication Accounting TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Incal FAP General Profilies 	Local Auth * The timeou used after al	n Active 1 It period di I Radius Se	Timeout ¹ (in su	ecs) EAP will always	i be]		

CLIから、次のコマンドを実行します。

(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60

show local-auth config コマンドを実行すると、このタイマーが設定されている値を確認できます。

(Cisco Controller) >show local-auth config

User credentials database search order: Primary Local DB

Timer:

Active timeout 60

Configured EAP profiles:

Name EAP-test

... Skip

9. 手動 PAC を生成およびロードする必要がある場合、GUI または CLI のいずれかを使用でき ます。GUI から、トップ メニューから [COMMANDS] を選択して、右側のリストから [Upload File] を選択します。[File Type] プルダウン メニューから [PAC (Protected Access Credential)] を選択します。すべてのパラメータを入力して、[Upload] をクリックします。

altala cisco			Sage Configuration Bing Logout Befree
Commands	Upload file from Controller	the Allerton Sconer, Blacker	Clear Upload
Download File	File Type	PAC (Protected Access Credential) 💌	
Reboot	User (Identity)	test1	
Reset to Factory Default Set Time	Validity (in days)	60	
	Password	•••••	
	Confirm Password	•••••	
	TFTP Server		
	IP Address File Path	10.1.1.1	
	File Name	, manual.pac	

(Cisco Controller) > transfer upload pac ?
username Enter the user (identity) of the PAC
(Cisco Controller) >transfer upload pac test1 ?
<validity> Enter the PAC validity period (days)</validity>
(Cisco Controller) >transfer upload pac test1 60 ?
<pre><password> Enter a password to protect the PAC</password></pre>
(Cisco Controller) >transfer upload pac test1 60 cisco123
(Cisco Controller) >transfer upload serverip 10.1.1.1
(Cisco Controller) >transfer upload filename manual.pac
(Cisco Controller) >transfer upload start
Mode.TFTPTFTP Server IP.10.1.1.1TFTP Path./TFTP Filename.manual.pacData Type.PACPAC User.test1PAC Validity.60 daysPAC Password.cisco123
Are you sure you want to start? (y/N) y PAC transfer starting. File transfer operation completed successfully.

Microsoft Certification Authority

EAP-FAST バージョン 2 および EAP-TLS 認証を使用するには、WLC およびすべてのクライアン ト デバイスが、有効な証明書を使用し、Certification Authority のパブリック証明書を認識する必 要があります。

設置

Windows 2000 サーバに Certification Authority サービスがインストールされていない場合はイン ストールする必要があります。

Windows 2000 サーバで Microsoft Certification Authority をアクティブにするには、次の手順を実行します。

1. コントロール パネルから、[Add/Remove Programs] を選択します。



2. 左側の [Add/Remove Windows Components] を選択します。



3. [Certificate Services] チェックボックスをオンにします。

Windows Components Wizard	×
Windows Components You can add or remove components of Windows 2000.	
To add or remove a component, click the checkbox. A part of the component will be installed. To see what's in Details.	shaded box means that only cluded in a component, click
Components.	121 MR
Costificate Services	1.4 MD
Certificate Services	
Internet Information Services (IIS)	21.6 MR
Apple and the services (IIS)	5 2 MD
Description: Installs a certification authority (CA) to issue public key security applications. Total disk space required: 0.0 MB Space available on disk: 4205.9 MB	e certificates for use with <u>D</u> etails
< <u>B</u> ack	<u>N</u> ext > Cancel
マの警告を確認して、次に進みます。	
1icrosoft Certificate Services	×
After installing Certificate Services, the computer cannot be renam from a domain. Do you want to continue?	ed and the computer cannot join or be removed
<u>Y</u> es <u>N</u> o	

4. インストールする Certification Authority のタイプを選択します。簡単なスタンドアロン認証 局を作成するには、[Stand-alone root CA] を選択します。

Certification Authority types:	Description:
 Enterprise root CA Enterprise subordinate CA Stand-alone root CA Stand-alone subordinate CA 	The most trusted CA in a CA hierarchy. Does not require Active Directory.

5. Certification Authority についての必要な情報を入力します。この情報は、Certification Authority の自己署名証明書を作成します。使用する CA 名を覚えておきます。Certification Authority は、証明書をデータベースに保存します。この例では、Microsoft により推奨され るデフォルト設定を使用します。

		Browse
		Bro <u>w</u> se
on 💦 a shared folder		
-0		
		Browse
	on 泽 a shared folder	on 泽 a shared folder

6. Microsoft Certification Authority サービスは、IIS Microsoft Web サーバを使用して、クライ アントおよびサーバ証明書を作成および管理します。この場合、IIS サービスを再起動する 必要があります。

Microsoft	: Certificate Services
⚠	Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?
	OK Cancel

Microsoft Windows 2000 サーバにより、新しいサービスがインストールされます。新しい Windows コンポーネントをインストールするには、Windows 2000 サーバ インストール CD が必要です。Certification Authority がインストールされます。

<u>Cisco Wireless LAN Controller での証明書のインストール</u>

Cisco Wireless LAN コントローラのローカル EAP サーバで EAP-FAST バージョン 2 および EAP-TLS を使用するには、次の 3 つの手順を実行する必要があります。

- 1. Wireless LAN Controller にデバイス証明書をインストールする。
- 2. <u>Wireless LAN Controller にベンダー CA 証明書をダウンロードする。</u>
- 3. EAP-TLS を使用するために Wireless LAN Controller を設定する。

このドキュメントの例では、Access Control Server(ACS)が Microsoft Active Directory および Microsoft Certification Authority と同じホストにインストールされていますが、ACS サーバが別の サーバにある場合でも設定は同じでなければなりません。

<u>Wireless LAN Controller でのデバイス証明書のインストール</u>

次のステップを実行します。

- 証明書を生成して WLC にインポートするには、次の手順を実行します。 http://<serverlpAddr>/certsrv に移動します。[Request a Certificate] を選択して、[Next] をク リックします。[Advanced Request] を選択して、[Next] をクリックします。[Submit a certificate request to this CA using a form] を選択してから [Next] をクリックします。 Certificate Template の [Web server] を選択して、関連する情報を入力します。次に、キー に exportable というマークを付けます。マシンにインストールする必要がある証明書を受け 取ります。
- 証明書を PC から受け取るには、次の手順を実行します。Internet Explorer ブラウザを開いて、[Tools] > [Internet Options] > [Content] を選択します。[Certificates] をクリックします。新しくインストールされた証明書をプルダウン メニューから選択します。[Export] をクリックします。[Next] を 2 回クリックして、[Yes export the private key] を選択します。このフォーマットは、PKCS#12(.PFX フォーマット)です。[Enable strong protection] を選択します。パスワードを入力します。ファイル <tme2.pfx> に保存します。
- 3. Openssl がインストールされている任意のコンピュータに PKCS#12 フォーマットで証明書 をコピーし、PEM フォーマットに変換します。

openssl pkcs12 -in tme2.pfx -out tme2.pem !--- The command to be given, -in Enter Import Password: !--- Enter the password given previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase. Verifying - Enter PEM pass phrase:

4. 変換後の PEM フォーマット デバイス証明書を WLC にダウンロードします。 (Cisco Controller) >transfer download datatype eapdevcert

(Cisco Controller) >transfer download certpassword password !--- From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download filename tme2.pem

(Cisco Controller) >transfer download start

Mode.TFTPData Type.Vendor Dev CertTFTP Server IP.10.1.1.12TFTP Packet Timeout.6TFTP Max Retries.10TFTP Path./TFTP Filename.tme2.pem

This may take some time. Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.

Reboot the switch to use new certificate.

5. 再起動したら、証明書を確認します。

(Cisco Controller) >show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer vendor CA certificate: Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT Device certificate: Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2 Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme

<u>Wireless LAN Controller へのベンダー CA 証明書のダウンロード</u>

次のステップを実行します。

- ベンダー CA 証明書を取得するには、次の手順を実行します。http://<serverlpAddr>/certsrv に移動します。[Retrieve the CA Certificate] を選択して、[Next] をクリックします。[CA Certificate] を選択します。[DER encoded] をクリックします。[Download CA certificate] を クリックして、証明書を rootca.cer として保存します。
- 2. openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM コマンドを使用して、DER フォーマットから PEM フォーマットにベンダー CA を変換します。出力ファイルは
 - 、PEM フォーマットの rootca.pem です。
- 3. ベンダー CA 証明書をダウンロードします。 (Cisco Controller) >transfer download datatype eapcacert

<filename> Enter filename up to 16 alphanumeric characters.

(Cisco Controller) >transfer download filename rootca.pem

(Cisco Controller) >transfer download start ?

(Cisco Controller) >transfer download filename ?

(Cisco Controller) >transfer download start

Mode.....TFTPData Type....Vendor CA CertTFTP Server IP....10.1.1.12TFTP Packet Timeout....6TFTP Max Retries....10TFTP Path...../TFTP Filename....rootca.pem

This may take some time. Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed. Reboot the switch to use new certificate.

<u>EAP-TLS を使用するための Wireless LAN Controller の設定</u>

次のステップを実行します。

GUI から、[Security] > [Local EAP] > [Profiles] を選択し、プロファイルを選択して、次のように 設定します。

- ・[Local Certificate Required]:オン
- [Client Certificate Required]:オン
- [Certificate Issuer] : [Vendor]
- [Check against CA certificates]:オン

iliilii cisco	MONITOR MIANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS HELP
Security	Local EAP Profiles > Edit	
* AAA General	Profile Name	EAP-test
+ RADIUS Authentication	LEAP	4
TACACS+	EAP-FAST	R
Local Net Users MAC Filtering	EAP-TLS	9
User Login Policies AP Policies	Local Certificate Required	P Enabled
* Local EAP	Client Certificate Required	R trabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor 💌
Priority Order	Check against CA certificates	P Enabled
Access Control Lists	Verify Certificate CN Identity	C Enabled
IPSec Certs		E
Wireless Protection Policies	Check Certificate Date Validity	C Enabled

<u>クライアント デバイスへの認証局証明書のインストール</u>

<u>クライアント用ルート CA 証明書のダウンロードとインストール</u>

クライアントは、ルート CA 証明書を Certification Authority サーバから取得する必要があります 。クライアント証明書を取得して、Windows XP マシンにインストールする方法はいくつかあり ます。有効な証明書を取得するには、Windows XP ユーザは、そのユーザ ID を使用してログイン し、ネットワーク接続を確立する必要があります。

Windows XP クライアントの Web ブラウザおよびネットワークの有線接続を使用して、プライベ ート ルート Certification Authority サーバからクライアント証明書を取得しました。この手順は Microsoft Certification Authority サーバからクライアント証明書を取得するために使用します。

- 1. クライアントの Web ブラウザを使用して、ブラウザで Certification Authority サーバを指定 します。これを行うには、http://IP-address-of-Root-CA/certsrv と入力します。
- 2. Domain_Name\user_name を使用してログインします。XP クライアントを使用するユーザのユーザ名を使用してログインする必要があります。
- 3. [Welcome] ウィンドウで、[Retrieve a CA certificate] を選択して、[Next] をクリックします。
- 4. [Base64 Encoding] および [Download CA certificate] を選択します。
- 5. [Certificate Issued] ウィンドウで、[Install this certificate] をクリックして、[Next] をクリッ クします。
- 6. [Automatically select the certificate store] を選択し、[Next] をクリックします。インポートの成功を示すメッセージが表示されます。
- 7. Certification Authority に接続して、Certificate Authority 証明書を取得します。

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
 Request a certificate
- Check on a panding contif
- Check on a pending certificate

Microsoft Certificate Services - tme

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

Choose file to download:



8. [Download CA certificate] をクリックします。

Microsoft Certificate Services - tme		Home
Retrieve The CA Certificate Or Certificate	Revocation List	
Install this CA certification path to allow your	computer to trust certificates issued from this certification	authority.
It is not necessary to manually install the CA	File Download - Security Warning	this certification authority, because the
CA certification path will be installed for you	Do you want to open or save this file?	
Choose file to download: CA Certificate: Currerz [tme]	Name: certnew.cer Type: Security Certificate, 798 bytes From: 10.1.1.12	
●DER encoded or ●Bar	Open Save Cancel	
Download CA certificate Download CA certification p Download latest certificate r	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>	

Next >

Hom

Certificate Import Wizard



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

ate	< Back Next > Cance
Cer	cate Store rtificate stores are system areas where certificates are kept.
WH (Automatically select the certificate store based on the type of certificate
	C Place all certificates in the following store
	Certificate store: Browse



9. Certification Authority 証明書が正しくインストールされているか確認するには、Internet Explorer を開き、[Tools] > [Internet Options] > [Content] > [Certificates] を選択します。



Internet Options 🛛 ? 🔀				
General Security Privacy Content Connections Programs Advanced				
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings				
Certificates				
Use certificates to positively identify yourself, certification authorities, and publishers.				
Clear SSL State Certificates Publishers				
Personal information				
AutoComplete stores previous entries AutoComplete				
Microsoft Profile Assistant stores your My Profile				
UK Cancel Apply				

[Trusted Root Certification Authority] に、新しくインストールした Certification Authority が 表示されます。

Thawte Server CA . Thawte Timestamping	12/31/2020	Thawte Server CA
. Thawte Timestamping		
	12/31/2020	Thawte Timesta
tme	2/28/2012	<none></none>
UTN - DATACorp SGC	6/24/2019	UTN - DATACorp
. UTN-USERFirst-Client	7/9/2019	UTN - USERFirst
. UTN-USERFirst-Hardw	7/9/2019	UTN - USERFirst
. UTN-USERFirst-Netwo	7/9/2019	UTN - USERFirst
. UTN-USERFirst-Object	7/9/2019	UTN - USERFirst
. VeriSign Commercial S	12/31/1999	VeriSign Commer
		Adver
. Remove		Advanc
ses		
	UTN - DATACorp SGC UTN-USERFirst-Client UTN-USERFirst-Hardw UTN-USERFirst-Netwo UTN-USERFirst-Object VeriSign Commercial S	UTN - DATACorp SGC 6/24/2019 UTN-USERFirst-Client 7/9/2019 UTN-USERFirst-Hardw 7/9/2019 UTN-USERFirst-Netwo 7/9/2019 UTN-USERFirst-Object 7/9/2019 VeriSign Commercial S 12/31/1999

<u>クライアント デバイス用のクライアント証明書の生成</u>

クライアントは、WLC で WLAN EAP-TLS クライアントを認証するために、Certification Authority サーバから証明書を取得する必要があります。クライアント証明書を取得して、 Windows XP マシンにインストールする方法はいくつかあります。有効な証明書を取得するには 、Windows XP ユーザは、そのユーザ ID を使用してログインし、ネットワーク接続(優先接続ま たは 802.1x セキュリティを無効にした WLAN 接続のいずれか)を確立する必要があります。

Windows XP クライアントの Web ブラウザおよびネットワークの有線接続を使用して、プライベ ート ルート Certification Authority サーバからクライアント証明書を取得しました。この手順は Microsoft Certification Authority サーバからクライアント証明書を取得するために使用します。

- 1. クライアントの Web ブラウザを使用して、ブラウザで Certification Authority サーバを指定 します。これを行うには、http://IP-address-of-Root-CA/certsrv と入力します。
- 2. Domain_Name\user_name を使用してログインします。XP クライアントを使用するユーザ のユーザ名を使用してログインする必要があります(ユーザ名は、クライアント証明書に組 み込まれます)。
- 3. [Welcome] ウィンドウで、[Request a certificate] を選択して、[Next] をクリックします。
- 4. [Advanced Request] を選択して、[Next] をクリックします。
- 5. [Submit a certificate request to this CA using a form] を選択してから [Next] をクリックしま

す。

- 6. [Advanced Certificate Request] フォームで、[Certificate Template] の [User] を選択し、[Key Size] に [1024] を指定して、[Submit] をクリックします。
- 7. [Certificate Issued] ウィンドウで、[Install this certificate] をクリックします。これにより、 クライアント証明書が Windows XP クライアントに正常にインストールされます。

Microsoft Certificate Services true	ome
Nelcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.	u
Select a task: ○ Retrieve the CA certificate or certificate revocation list ③ Request a certificate ○ Check on a pending certificate	
Next >	ן
Microsoft Certificate Services tme	lome
Choose Request Type	
Please select the type of request you would like to make:	
User Certificate request: User Certificate	
 Advanced request 	
Next >)
Microsoft Certificate Services tme	ome
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certificat authority (CA) will determine the certificates that you can obtain.	tion
 Submit a certificate request to this CA using a form. 	
 Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file. 	
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrolment event certificate to submit a request for another user. 	

Next >

8. [Client Authentication Certificate] を選択します。

Microsoft Certifi	cate Services tme
Advanced Ce	rtificate Request
Certificate Tem	plate:
	User
Key Options:	
CSP:	Microsoft Base Cryptographic Provider v1.0
Key Usage:	○Exchange ○Signature ④Both
Key Size:	512 Min: 384 (common key sizes: 512 1024) Max: 1024
	Create new key set Set the container name Use existing key set
	Enable strong private key protection
	Mark keys as exportable
	Use local machine store You must be an administrator to generate a key in the local machine store.
Additional Optic	ins:
Hash Algorithm:	SHA-1 Only used to sign request.
	Save request to a PKCS #10 file
Attributes	

証明書が作成されます。

9. 証明書がインストールされているか確認するには、Internet Explorer を開き、[Tools] > [Internet Options] > [Content] > [Certificates] を選択します。[Personal] タブに証明書が表示 されます。

Certificates					?	×
Intended purpo	ose:	<ali></ali>				<
Personal Ot	her Peop	le Intermediate Certificati	on Authorities Trust	ed Root Certificatio	r <	>
Issued To		Issued By	Expiratio	Friendly Name		
🕮 Adminis	trator	tme	3/27/2008	<none></none>		
Import Certificate int Encrypting Fil	Exp tended pu le System	ort Remove Irposes , Secure Email, Client Authe	entication	Advan View Clo	ced	

<u>クライアント デバイス上での Cisco Secure Services Client による EAP-TLS の指定</u>

次のステップを実行します。

- デフォルトでは WLC は SSID をブロードキャストするため、その SSID が、スキャンされ た SSID の [Create Networks] リストに表示されます。Network Profile を作成するには、 [Enterprise] リストの [SSID] をクリックし、[Create Network] をクリックします。WLAN イ ンフラストラクチャでブロードキャスト SSID が無効にされている場合、SSID を手動で追 加する必要があります。これを行うには、[Access Devices] で [Add] をクリックして、適切 な SSID (たとえば、Enterprise)を入力します。 クライアントのアクティブ プローブ動作 を設定します。これで、クライアントがアクティブに設定済み SSID をプローブします。 [Add Access Device] ウィンドウで [SSID] を入力したら、[Actively search for this access device] を指定します。注: EAP認証設定がプロファイルに対して最初に設定されていない 場合、ポート設定ではエンタープライズモード(802.1X)は許可されません。
- 2. [Create Network] オプション ボタンを押すと [Network Profile] ウィンドウが表示され、この ウィンドウでは選択済み(または設定済み)の SSID を認証メカニズムとアソシエーション することができます。プロファイルに説明的な名前を割り当てます。**注:この**認証プロファ

イルでは、複数のWLANセキュリティタイプまたはSSIDを関連付けることができます。

- 🗆 ×

Cisco Secure Services Client

Client Administration Help

Access 🛆	Data Security
aruba-ap-config-in-the-clear (2 accesses dete	省 WEP
il b	💢 Open
ccx5 (2 accesses detected)	💢 Open
con	💢 Open
n con-eap	WEP
001907351aa3 High Signal	WEP
guestnet (5 accesses detected)	💢 Open
guestnetwork	💢 Open
N-Rogue	WEP WEP
secure-1 (3 accesses detected)	? Mixed
tme-test (5 accesses detected)	🖀 WPA
trng1 (2 accesses detected)	🚡 WEP
Create Netw	ork

- 3. 認証を有効にして、EAP-TLS 方式を確認します。次に、[Configure] をクリックして、[EAP-TLS] プロパティを設定します。
- 4. [Network Configuration Summary] の下で [Modify] をクリックして EAP/クレデンシャルを設 定します。
- 5. [Turn On Authentication] を指定し、[Protocol] で [EAP-TLS] を選択して、[Identity] で [Username] を選択します。
- 6. ネットワーク認証用のログオン クレデンシャルを使用するには、[Use Single Sign on Credentials] を指定します。[Configure] をクリックして EAP-TLS のパラメータを設定しま す。

Network Authentication	×
Network Authentication Network: con-eap Network Authentication Methods:	User Credentials: C Use Machine Credentials Use Single Sign on Credentials Request when needed Remember forever Remember for this session Remember for 5 minutes
EAP-TLS FAST GTC Configure	
Help	OK Cancel

etwork Profile					
Vetwork					
Name: con-eap N	etwork				-
🔽 Availat	ble to all users (pu	blic profile)			
T Autom	atically establish M	achine conn	ection		
Autom	atically establish L	Jser connecti	on		
	Before user accor	unt (supports :	smartcard	l/password only)	
Network Configurati	on Summary:				
Authentication:	AP-TLS:				٦
Condensidor L					╡
Credentials:	fequest when ne	eded and rem	ember for	the session.	
				Modify	
					-
Access Devices					_
Access / SSID	Mode	Notes			
con-eap	WPA2 Enterpri	se			
	1 11-11-1	Canfinuation		Demand	
Add	Modify	Configuration.		Remove	
Add	Modify	Configuration.		Remove	

7. EAP-TLS を安全に設定するには、RADIUS サーバ証明書を確認する必要があります。これ を行うには、[Validate Server Certificate] チェックボックスをオンにします。

Configure EAP Metho	id	×
-EAP-TLS settings:		
Use Smartcard-base	d Client Certificates Only	
Validate Server Cert	ificate	
Allow Fast Session F	Resumption	
]
Help	ΟΚ	Cancel

8. RADIUS サーバ証明書を検証するには、Cisco Secure Services Client 情報を提供して、正しい証明書だけを取得する必要があります。[Client] > [Trusted Servers] > [Manage Current User Trusted Servers] を選択します。

Cisco Secure Services	Client	
Client Administration Help		
Manage Adapters	a Mahuarka	
Trusted Servers 🔸	Manage Current User Trusted Serv	vers
Advanced Settings	Manage Machine / All Users Truste	d Servers Data Seci
Enable Client Turn WiFi Radio On	ork Disconnected	
Show System Trav	Misconfigured A	ccess (AutoConnect) 🕋 WPA
Close Window	Capable for: Configured f	wep for wpa2
. ■	Configure Bernove	Details
	Conliguie	
🜑 Manage Current User 🕯	Trusted Servers	X
-Trusted Server Definition -	Current Hears	
	· Culteric Osels.	
Rule Name		Validation Method
1110 01	Domous Coloriad	E Ji Calastal
Add Server Rule	Hemove Selected	Edit Selected
Add Server Rule	Fremove Selected	E dit Selected

9. ルールに名前を付けて、サービス証明書の名前を確認します。

Trusted Server	
Trusted Server	
Rule name: WLC-Config	
Validation method: Certificate	•
Match ANY Certificate Validation Rule:	<u>v</u>
Subject/Common Name Exactly matches	tme
L	
Help	OK Cancel

EAP-TLS 設定は終了です。

10. ワイヤレス ネットワーク プロファイルに接続します。Cisco Secure Services Client により、ユーザ ログインが求められます。

Cisco Secure Services Client	
Client Administration Help	
Create Networks Manage Networks	
Network	
Con Net Con Con-eap Con-eap Con-eap Con-eap Con-eap Con-eap Con-eap Con-eap Con-eap Con-eap Con-eap	als for , access con-eap
Send Ca	incel
Connect Configure Remove	Status

sco Secure Services Client は、サーバ証明書を受け取り、これを確認します(ルールが設 定され、Certification Authority がインストールされている場合)。 ユーザに使用する証明

書を求められます。

11. クライアントが認証を行った後、接続の詳細情報を照会するには、[Manage Networks] タ ブの [Profile] の下で [SSID] を選択し、[Status] をクリックします。[Connection Details] ウ ィンドウには、クライアント デバイス、接続の状態と統計、および認証方式に関する情報 が表示されます。[WiFi Details] タブには、802.11 の接続状態に関する詳細情報が表示され ますが、これには RSSI、802.11 チャネル、および認証/暗号化が含まれます。 xI

_	_	
	Concession in the local division of the loca	

Selected Acce	\$\$	Status		Security
con-eap		Connected: Authenticated	(AutoConn \	WPA2
1:24:28.044	con-eap Network Cor	nnection requested from use	r context.	
1:24:28.054	Connection authentica	ation started using the logger	d in user's crede	initials.
1:24:28.074	Port state transition to.	AL_PURI_STATE_UNAU	HENTICATED	AL_PURI_STATUS_STARTED
1.24.20.034	Connection association	n started using enclyption mo	DOB AU_ENCH_	AES AC_ASSUC_11[0021A
1-24-28 194	Port state transition to	AC PORT STATE CONNE	CTINGIAC PO	IRT STATUS LINK LIPI
1:24:28.295	Port state transition to	AC PORT STATE AUTHE	NTICATINGIA	C PORT STATUS 8021x ACQUIRED
1:24:28.305	Identity has been requ	ested from the network.		
1:24:28.315	315 Identity has been sent to the network. 335 Authentication started using method type EAP-TLS, level 0			
1:24:28.335				
1:24:28.335	The server has reques	sted using authentication typ	e: EAP-TLS	
1:24:28.335	The client has request	ted using authentication type	: EAP-TLS	
1:24:28.395	Validating the server.			CODT ATATUS COOLD KOS
1:24:28.505	Port state transition to.	AC_PURI_STATE_AUTHE	NTICATEDIAC	_PURT_STATUS_GROUP_KEY)
1:24:20.505	The following IP addre	are has been accired. 10.1	0 90 24	
1.24.55.554	The following in addre	ss has been assigned. To h	0.00.24.	
		~		
		Clear		

Cisco Secure Services Client	
Create Networks Manage Networks	
Network 🛆	Status Data :
E- Con Network	Disconnected
Con	No Adapter Available (Suspended) 🛛 🗕 🕅
- 🐑 con-eap Network	Connected: Authenticated
L	Connected: Authenticated (AutoConnect) 🗃 🛝
•	•
	Details
Disconnect Configure	Remove Status

onnection Status	Details
Status:	Connected: Authenticated
Duration:	00:01:19
Network Profile:	con-eap Network
Network Adapter:	Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:	00-40-96-A6-D6-F6
Access Device:	con-eap
Access Device MAC Add	ress: 00-19-07-35-1A-AC
Transmitted packets:	346
Received packets:	3
Speed:	54.0 Mbps
Authentication Method:	EAP-TLS
Authentication Server:	tme2 (trusted)
IP Address:	10.10.80.24
Help	Close

<u> デバッグ コマンド</u>

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

注:debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

認証交換の進行状況を監視するために、WLC では次の debug コマンドが使用できます。

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable
- ・debug aaa local-auth eap events enableまたは

• debug aaa all enable

<u>関連情報</u>

- <u>Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 4.1</u>
- •<u>WLAN に関する技術サポート</u>
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>